

Инструкция по подключению к АСОИ ФинЦЕРТ

Порядок подключения к АСОИ ФинЦЕРТ на примере использования ПО Континент TLS-клиент описан в документе «Руководство Участника по работе с АСОИ ФинЦЕРТ», размещенном на портале АСОИ ФинЦЕРТ в разделе АСОИ ФинЦЕРТ (Документация и ПО Участника) (https://portal.fincert.cbr.ru/Content/1136/руководство_участника.pdf). Также Участникам настоятельно рекомендуется ознакомиться с документацией производителя на используемое Средство криптографической защиты информации (СКЗИ).

Для доступа к АСОИ ФинЦЕРТ необходимо:

– при работе с СКЗИ Континент TLS-клиент:

1. запустить Континент TLS-клиент;
2. использовать один из поддерживаемых АСОИ ФинЦЕРТ обозревателей:
 - Microsoft Edge;
 - Google Chrome версии не ниже 60;
 - Яндекс.Браузер версии не ниже 22;
 - Опера версии не ниже 83;
 - Chromium-Gost версии не ниже 99.

– при работе с СКЗИ КриптоПро:

1. использовать один из поддерживаемых АСОИ ФинЦЕРТ обозревателей:
 - Microsoft Edge;
 - Яндекс.Браузер версии не ниже 22;
 - Опера версии не ниже 83;
 - Chromium-Gost версии не ниже 99 (при использовании КриптоПро CSP 4.0 рекомендуется перейти на КриптоПро CSP 5.0).

1. Получение, установка и настройка СКЗИ «Континент TLS-клиент»

1.1. СКЗИ «Континент TLS-клиент» **может** использоваться для организации защищенного канала подключения к АСОИ ФинЦЕРТ, также оно **необходимо** для подготовки заявки на получение пользовательского TLS-сертификата. *(При использовании в компании СКЗИ КриптоПро, для формирования заявки на TLS-сертификат необходимо использовать ПО «Континент TLS-клиент», которое в таком случае следует устанавливать поверх КриптоПро, что позволит задействовать криптопровайдер разработки компании КриптоПро. Если Вы используете СКЗИ КриптоПро и у вас уже имеются готовые пользовательские TLS-сертификаты, то следует перейти к п.2 данной инструкции).*

Для получения СКЗИ «Континент TLS-клиент» необходимо зарегистрироваться на сайте производителя – компании «Код безопасности» (www.securitycode.ru), см. рис.1.

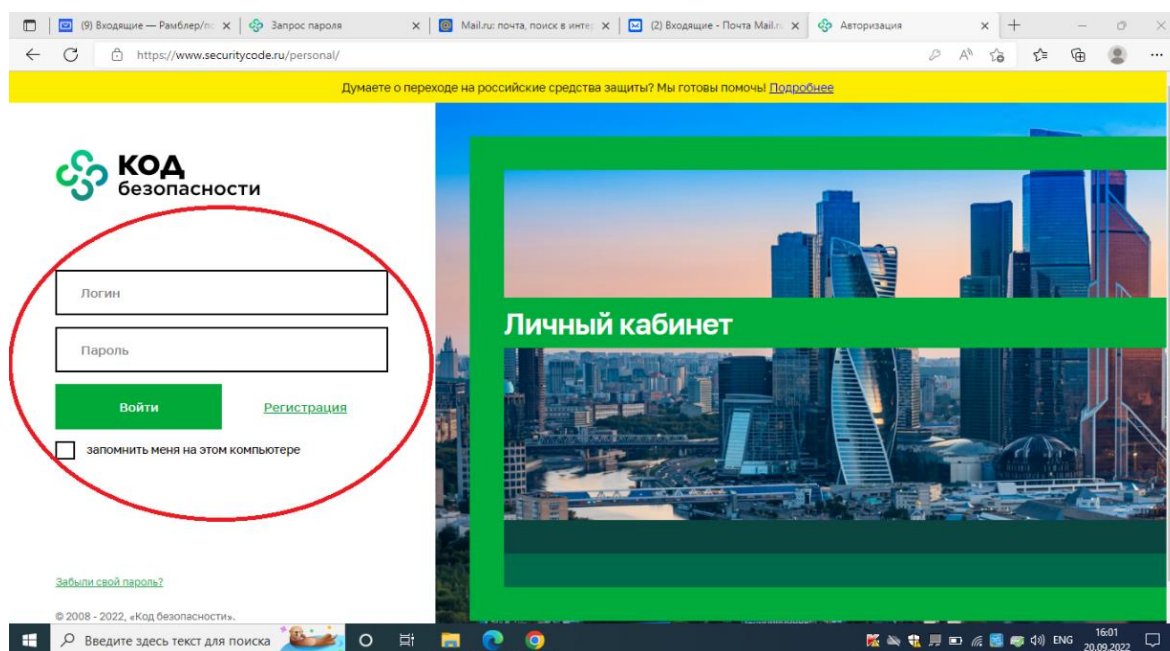


Рис.1

После успешной регистрации, на почтовый адрес, указанный при регистрации, поступит сообщение с кодом для подтверждения регистрации.

1.2. Далее необходимо авторизоваться на сайте и перейти в раздел «Продукты», см. рис.2.

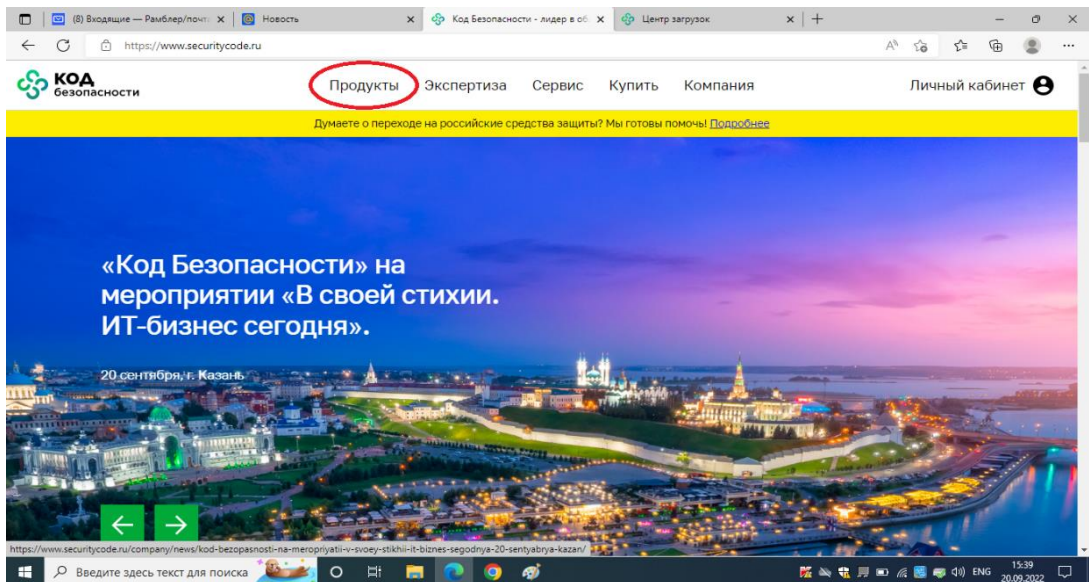


Рис.2

1.3. В разделе «Продукты» выбрать из списка «Континент TLS», см. рис.3.

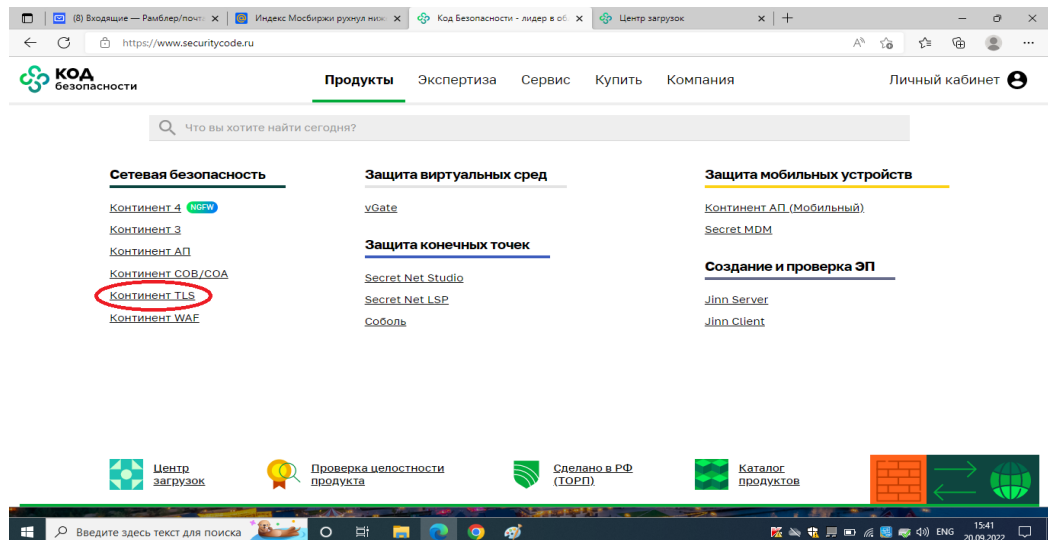


Рис.3

1.4. Далее выбрать «Скачать демо», см. рис.4.

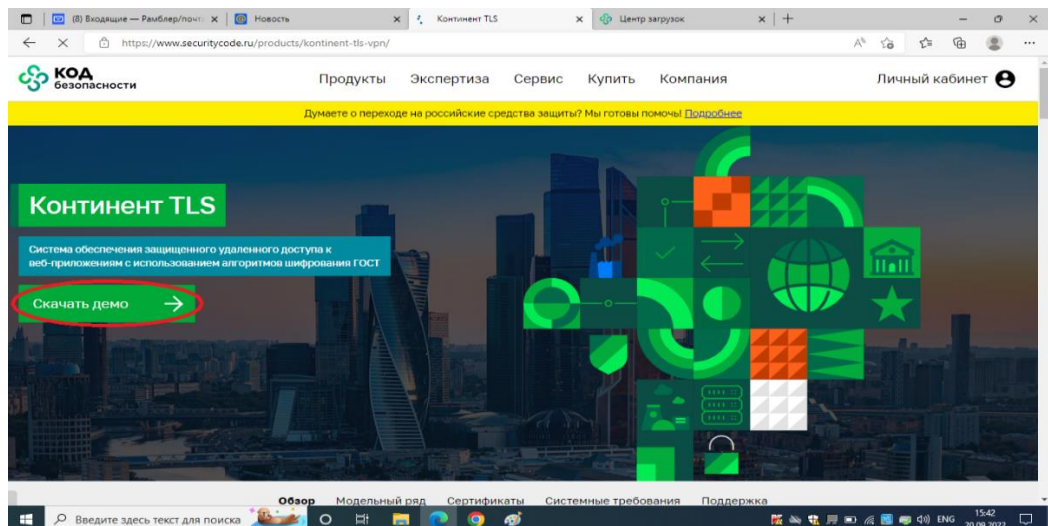


Рис.4

1.5. Скачать демоверсию Континент TLS-клиент, см. рис.5

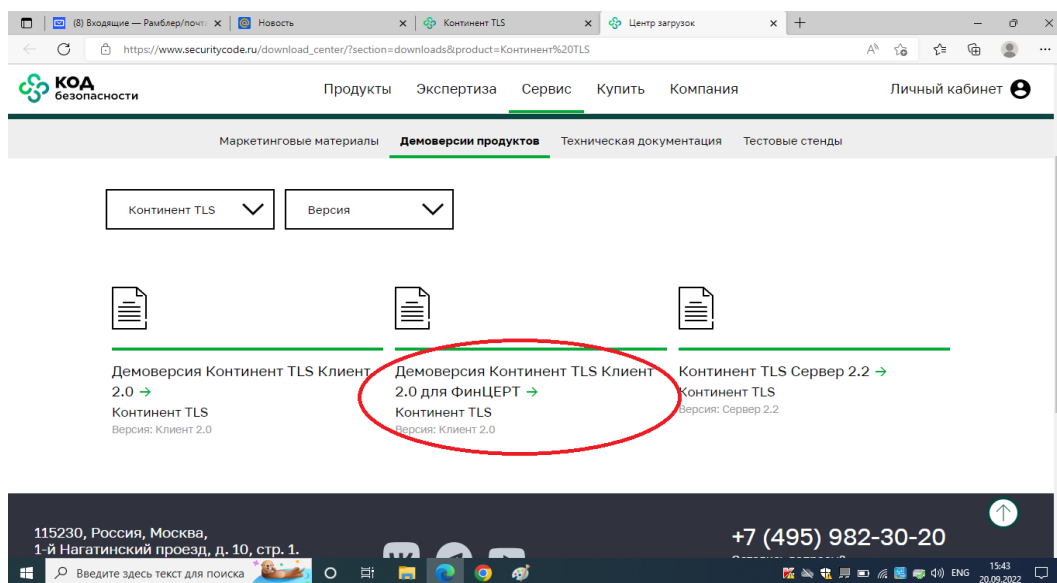


Рис.5

1.6. Разархивировать скаченный архив с дистрибутивом СКЗИ «Континент TLS-клиент». Рекомендуется производить установку ПО под пользователем с правами «Администратор» или административной УЗ.

1.7. Запустить установщик СКЗИ «Континент TLS-клиент», см. рис.6.

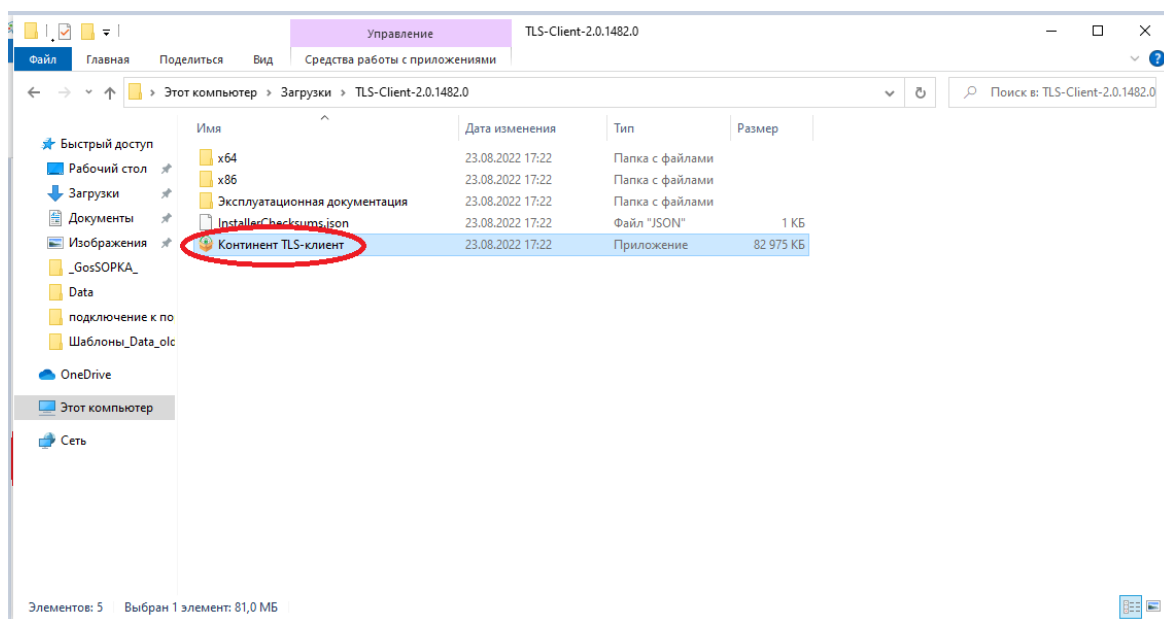


Рис.6

1.8. В следующем диалоговом окне проставить отметку, как показано на рис.7 и нажать «Установить».

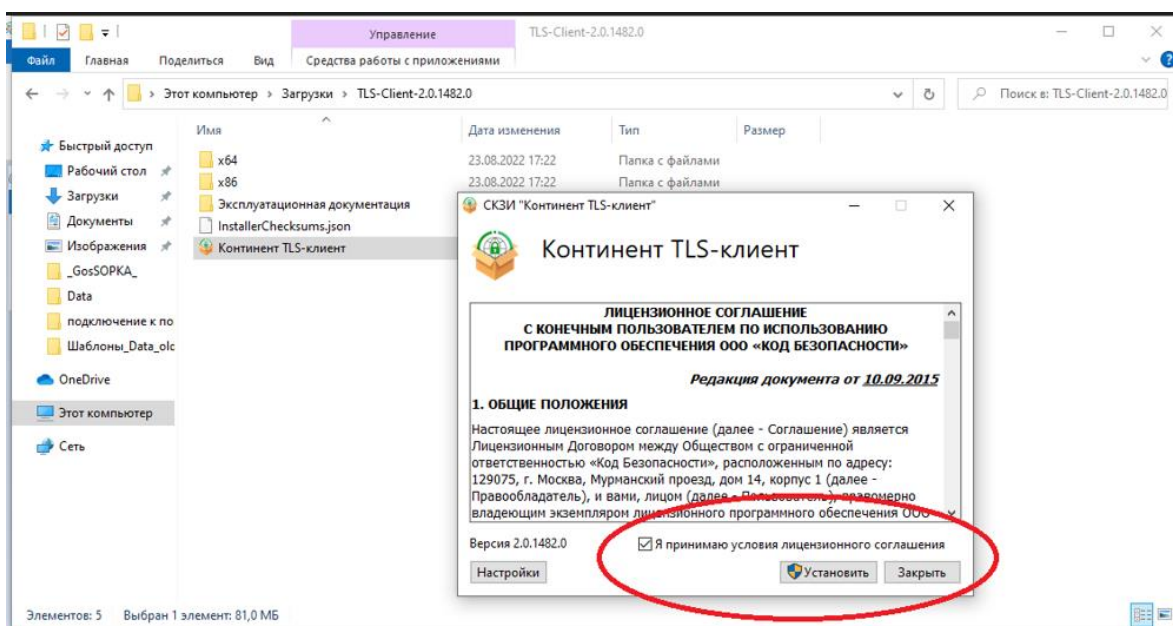


Рис.7

1.9. После установки СКЗИ «Континент TLS-клиент» перезагрузить ПК, см. рис.8.

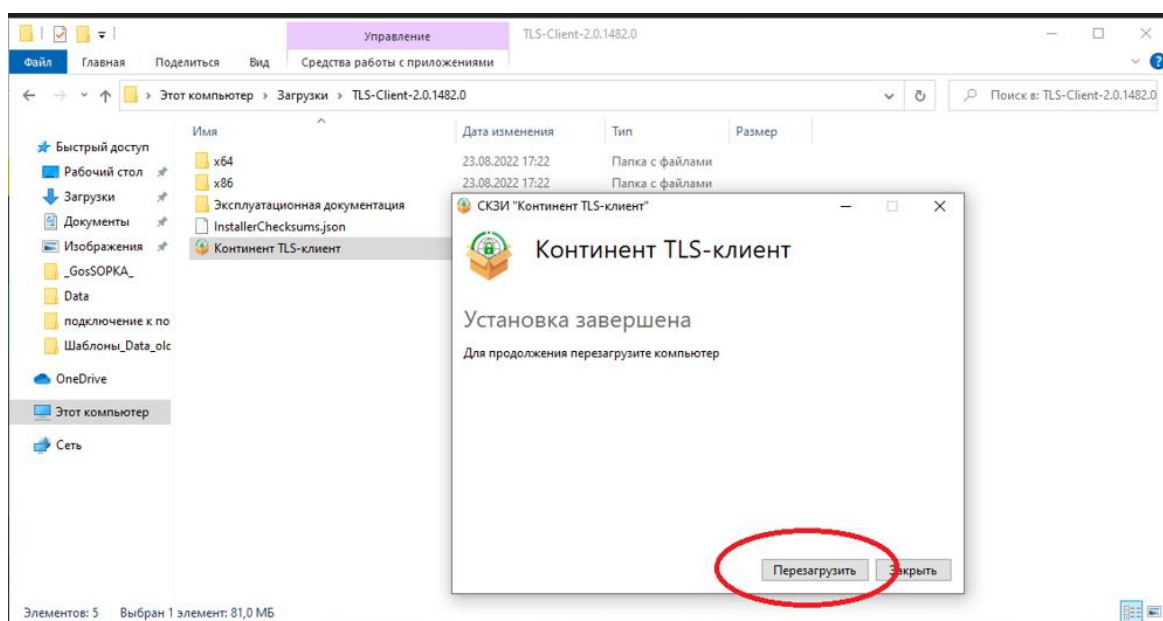


Рис.8

1.10. Для дальнейшей установки необходимо пройти биологический датчик случайных чисел (необходимо кликать левой кнопкой «мыши» по всем шарикам), см. рис.9.

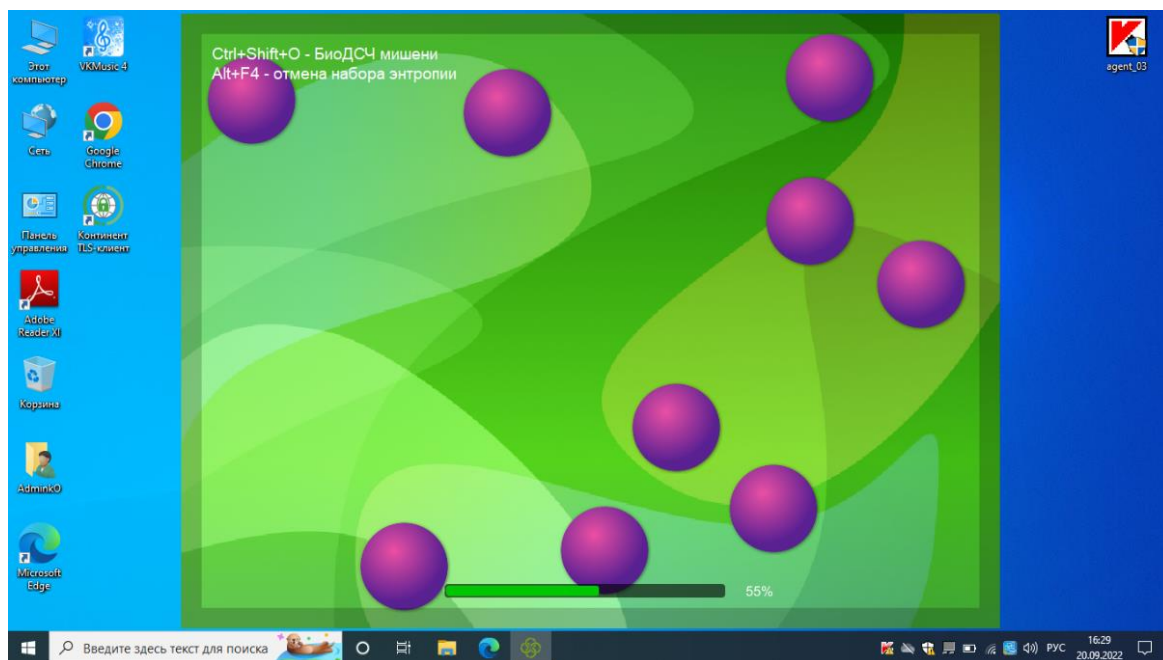


Рис.9

2. После завершения установки СКЗИ «Континент TLS-клиент» необходимо установить корневой и серверные сертификаты (сертификаты ресурсов в сети Интернет) в операционную систему. Сертификаты размещаются на информационном портале АСОИ ФинЦЕРТ (portal.fincert.cbr.ru) в разделе «АСОИ ФинЦЕРТ (Документация и ПО Участника)». При первоначальном подключении сертификаты направляются дежурной службой ФинЦЕРТ (info_fincert@cbr.ru, +7 (495) 772-70-90).

2.1. Для установки сертификата необходимо открыть файл, в открывшемся окне нажать кнопку «Установить сертификат». В окне «Мастера импорта сертификатов» в поле «Расположение хранилища» выбрать «Локальный компьютер». В этом случае сертификат установится для всех учетных записей (УЗ) пользователей операционной системы. Корневой сертификат устанавливается в хранилище «Доверенные корневые центры сертификации», серверные сертификаты – в «Доверенные издатели», см. рис. 10-14.

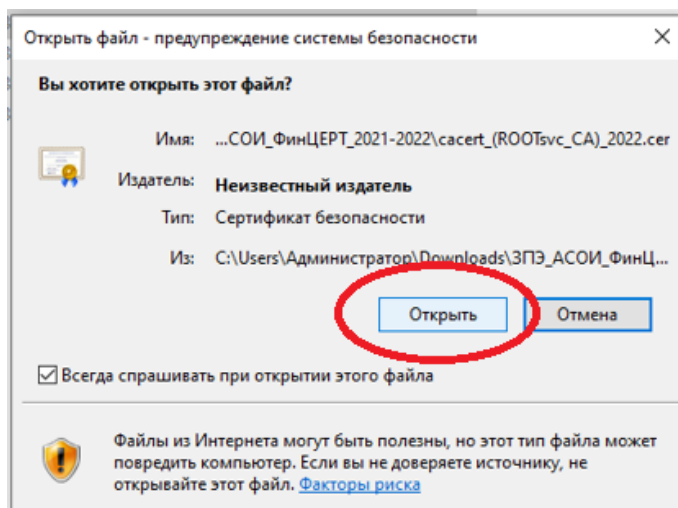


Рис.10

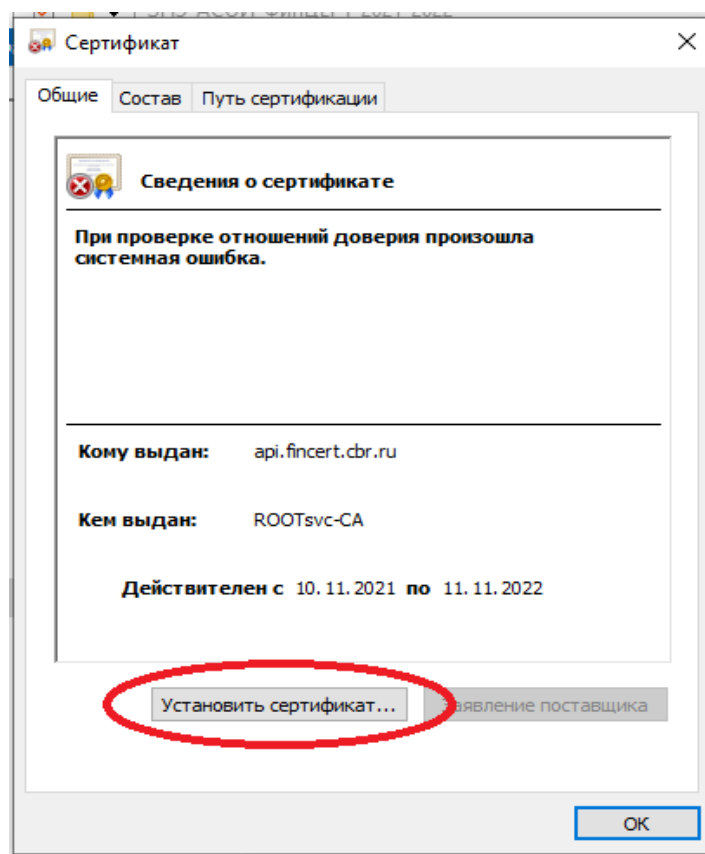


Рис.11

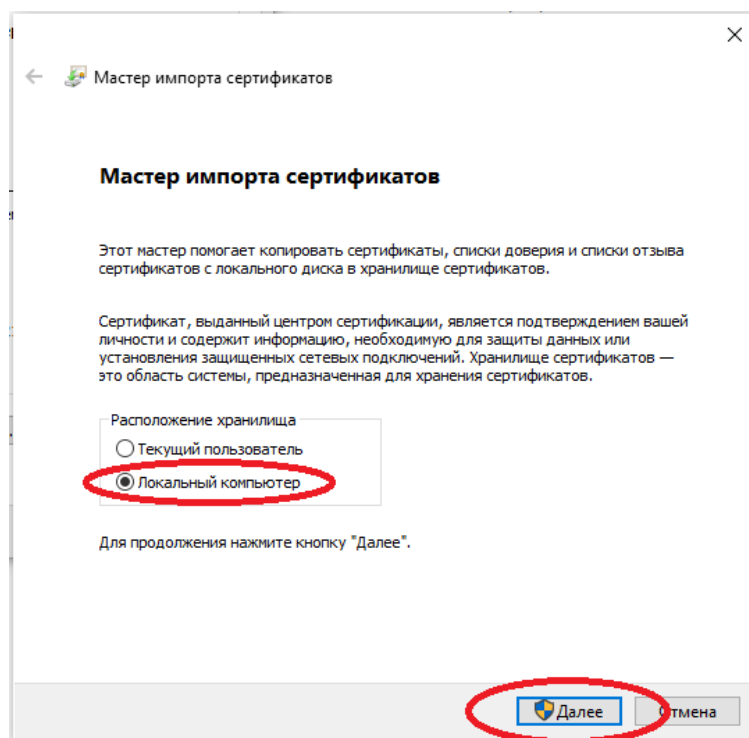


Рис.12

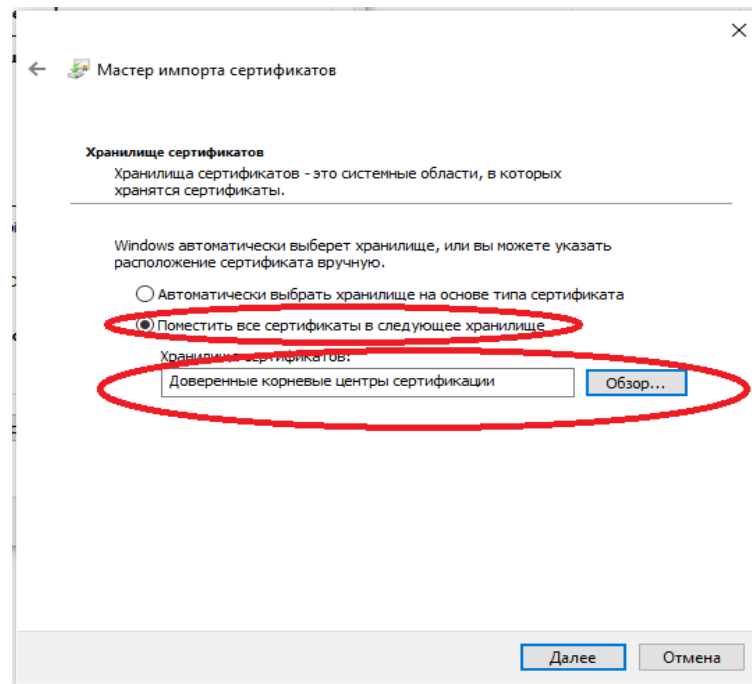


Рис.13

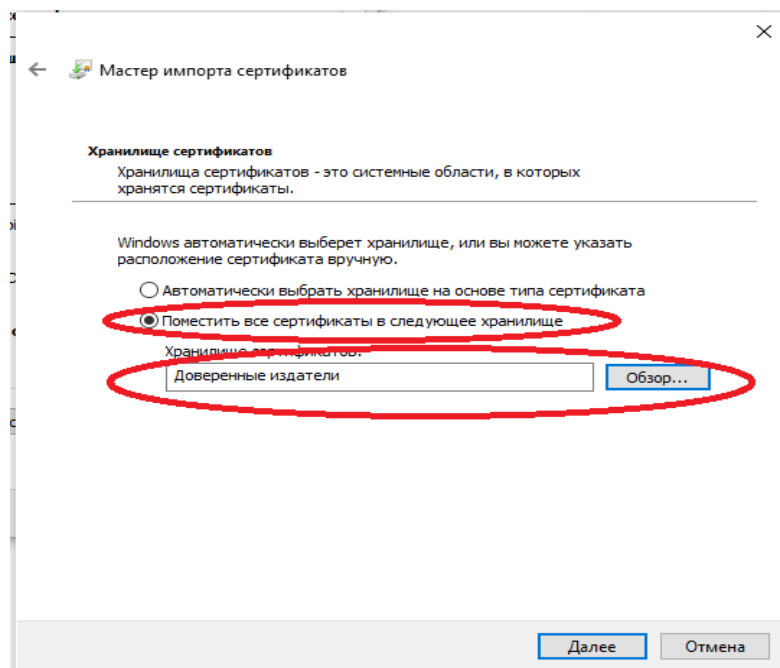


Рис.14

2.2. В процессе установки корневого сертификатов появится «Предупреждение системы безопасности». Нажмите «Да» и после установки «Готово», см. рис.15.

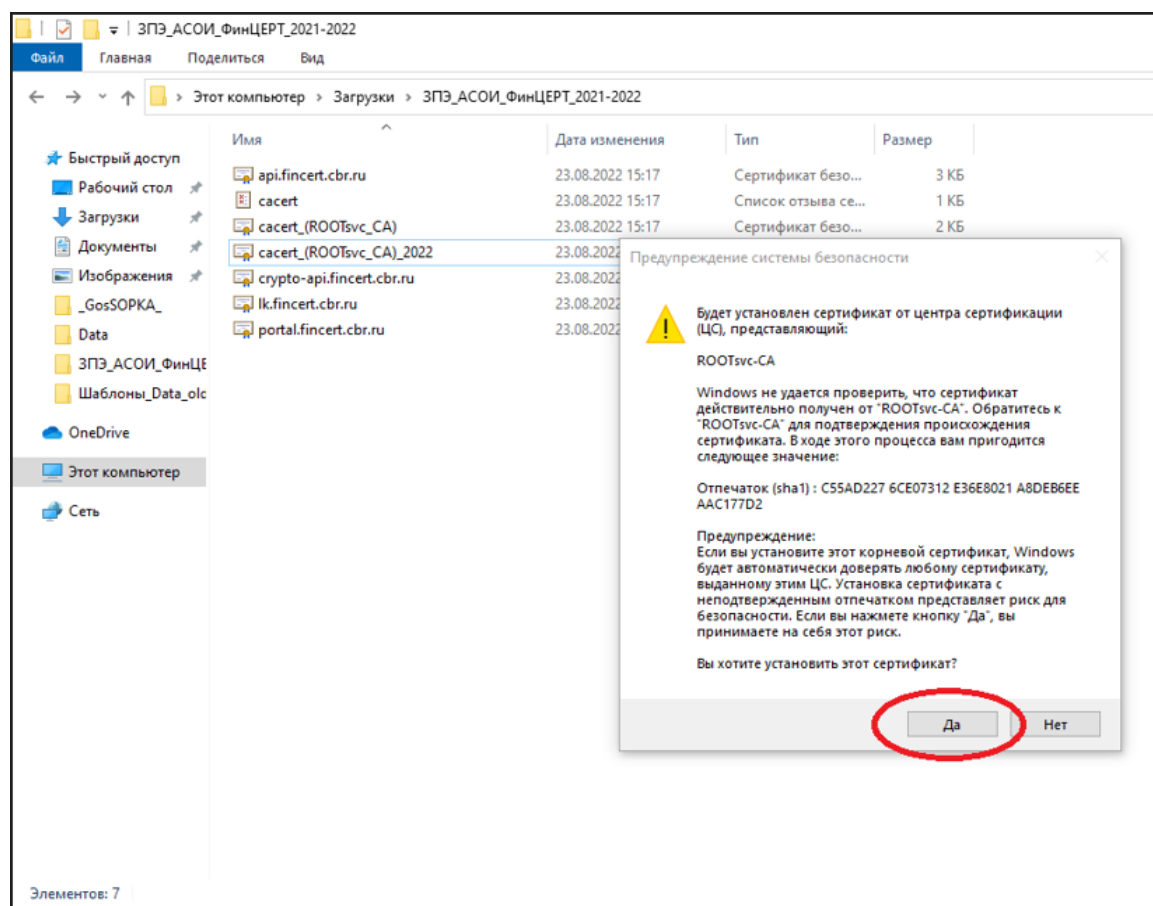


Рис.15

3. После установки корневого и серверных сертификатов, открыть СКЗИ «Континент TLS-клиент». Если на вкладке «Серверные сертификаты» не отображаются ранее установленные сертификаты, то необходимо их импортировать. Нажать кнопку «Импортировать», выбрать корневой сертификат `cacert_(ROOTsvc_CA).cer` и нажать «Открыть». Далее также импортировать остальные сертификаты. После завершения импорта сертификатов нажать кнопку «Обновить». Если все сертификаты установились и импортировались корректно, то статус сертификатов будет «Действителен», см. рис.16-18.

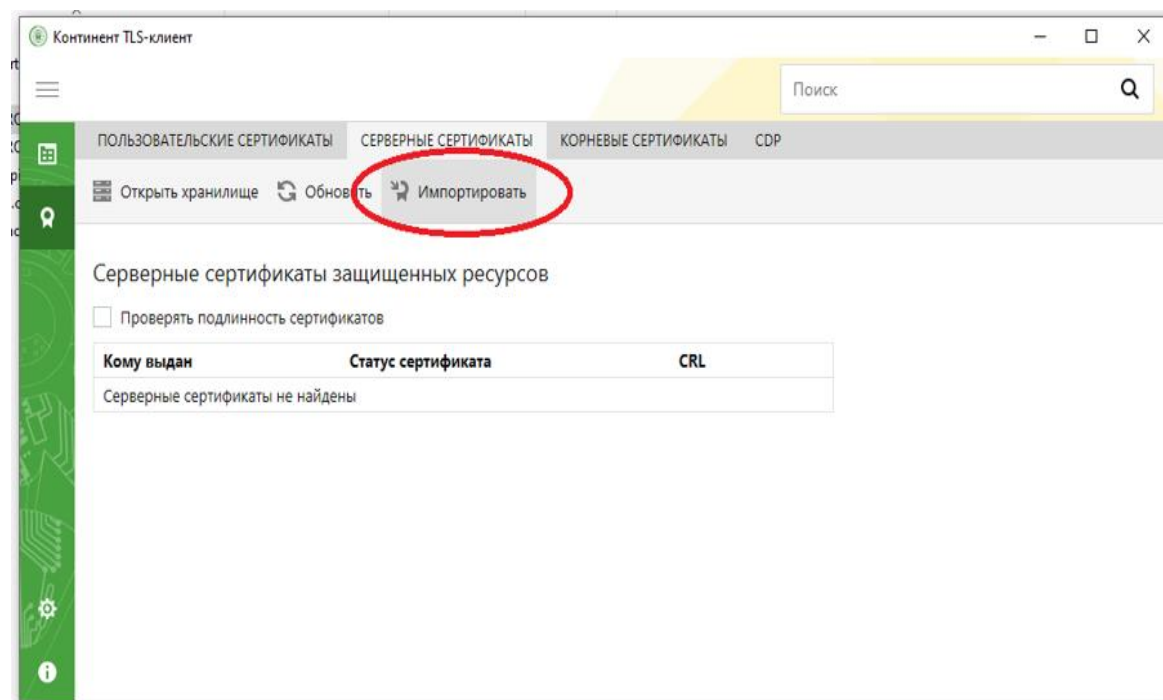


Рис.16

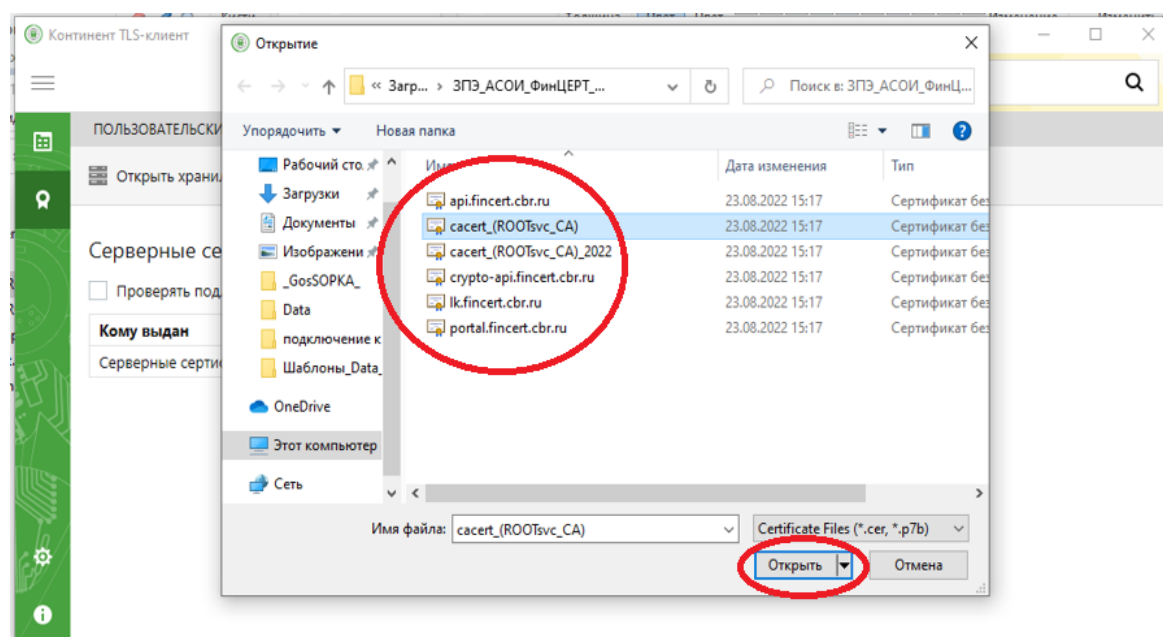


Рис.17

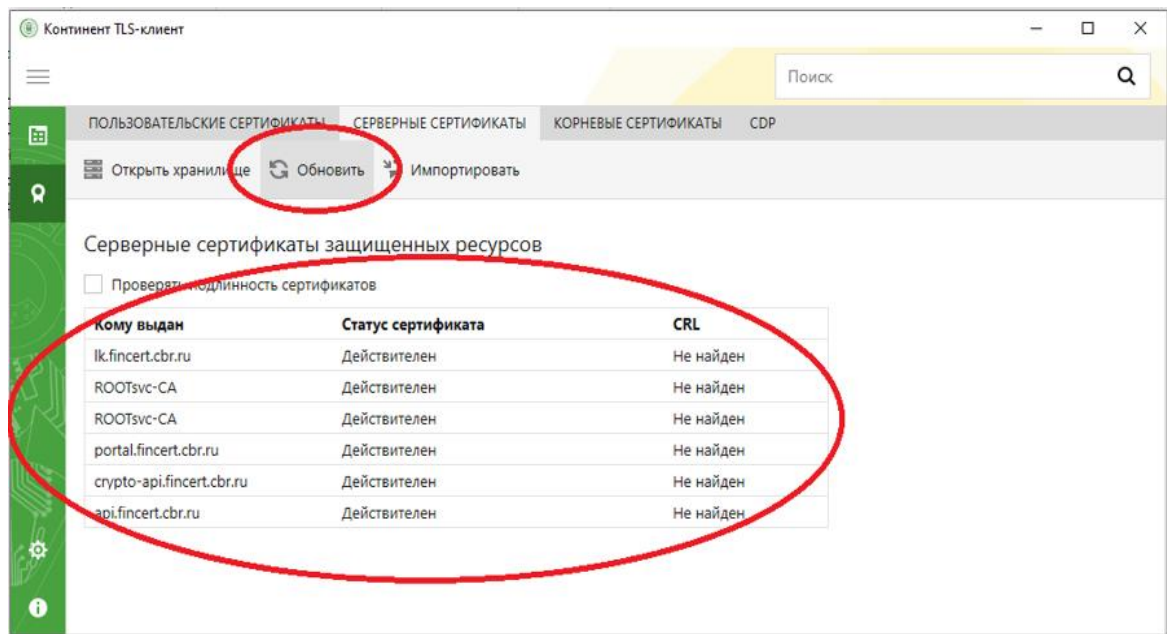


Рис.18

4. Далее необходимо добавить ресурсы АСОИ ФинЦЕРТ. Это можно сделать двумя способами:

- 1) импортированием файла конфигурации через «Настройки», см. рис.19. Файл конфигурации входит в комплект файлов вместе с корневым и серверными сертификатами (conf.json);
- 2) добавлением вручную (указать значения полей), см. рис.20.

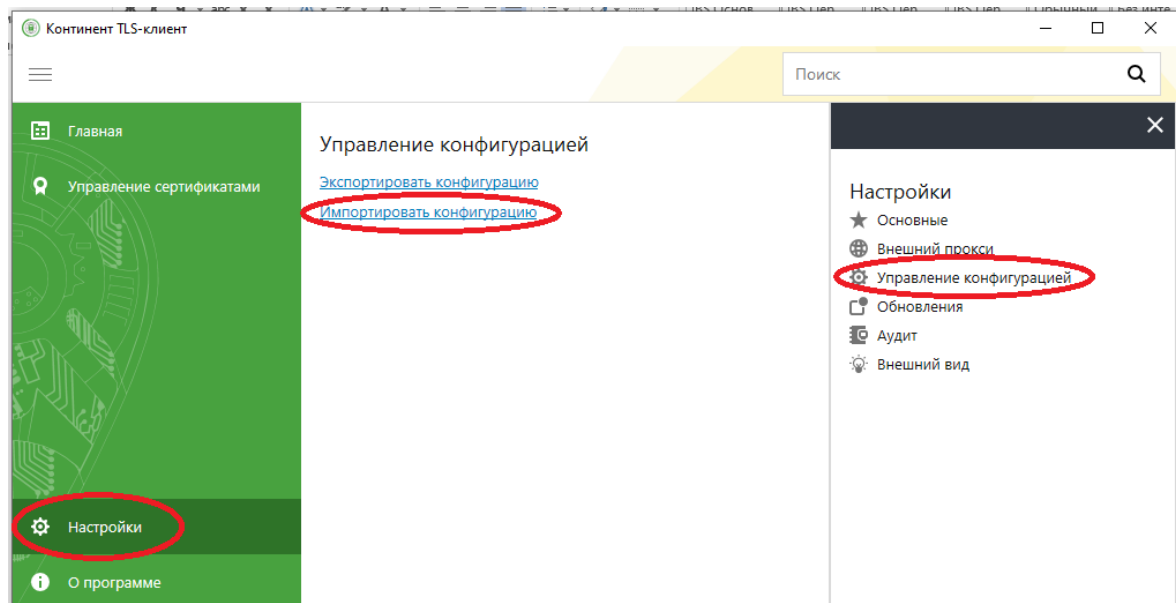


Рис.19

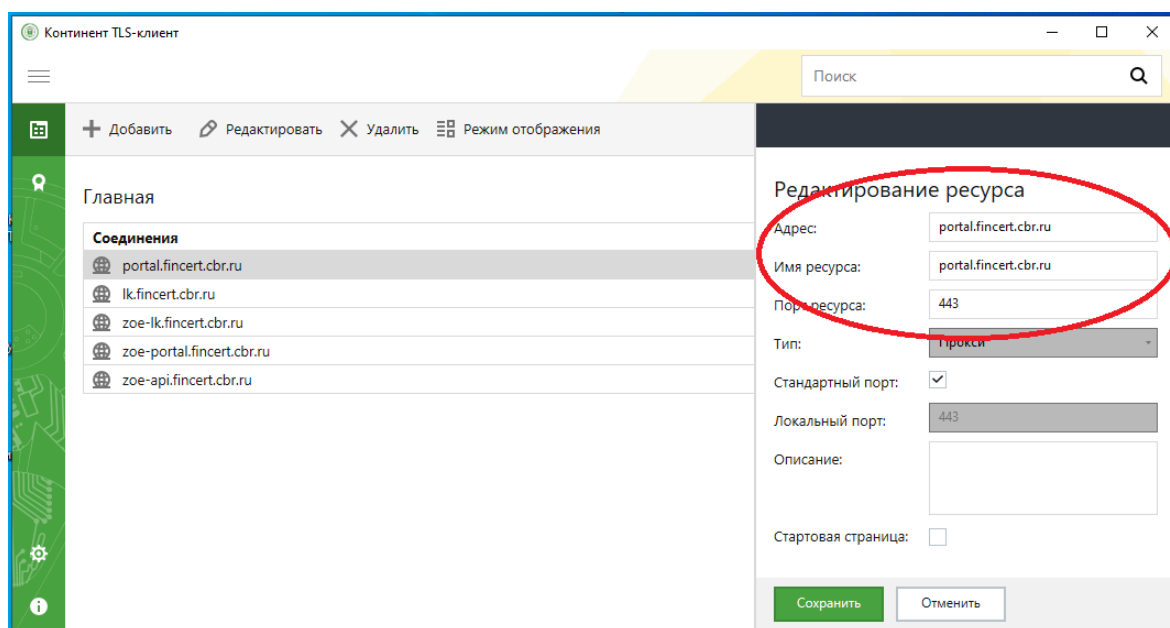


Рис.20.

4.1. После добавления ресурсов необходимо убедиться, что в настройках не стоит отметка «Проверить сертификат по CRL», см. рис.21.

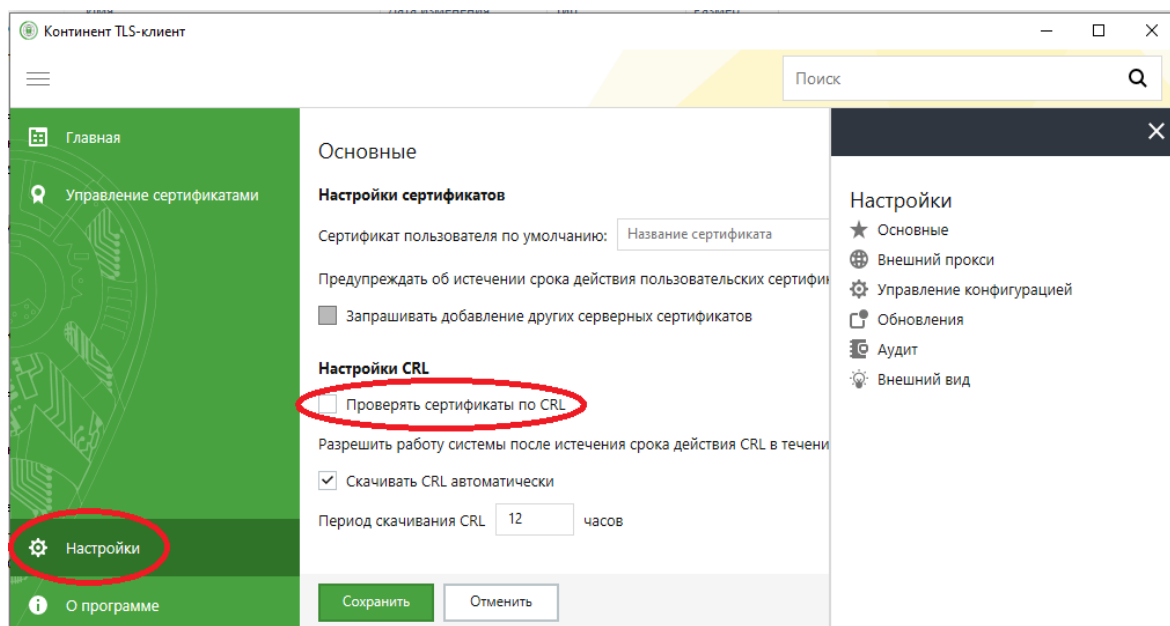


Рис.21

При выполнении всех шагов в строгой последовательности Вы сможете зайти на информационный портал АСОИ ФинЦЕРТ, см. рис.22.

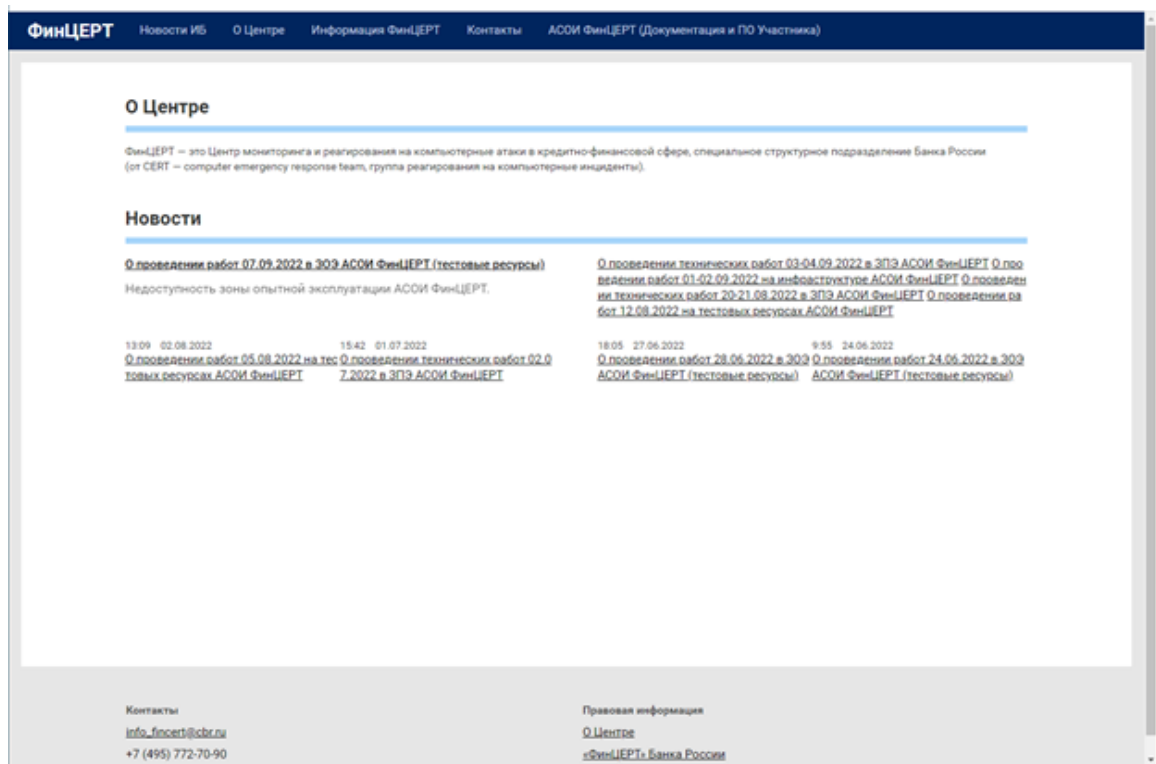


Рис.22

**Генерация закрытого ключа и формирование запроса
на получение сертификата в СКЗИ Континент TLS-клиент
(с использованием штатного криптопровайдера Код Безопасности CSP)**

5. Открыть СКЗИ «Континент TLS-клиент». Перейти в раздел «Управление сертификатами» и на вкладке «Пользовательские сертификаты» нажать «Создать запрос», в открывшемся окне нажать «Далее» (выбрать «Произвольный тип»), см. рис.23-24.

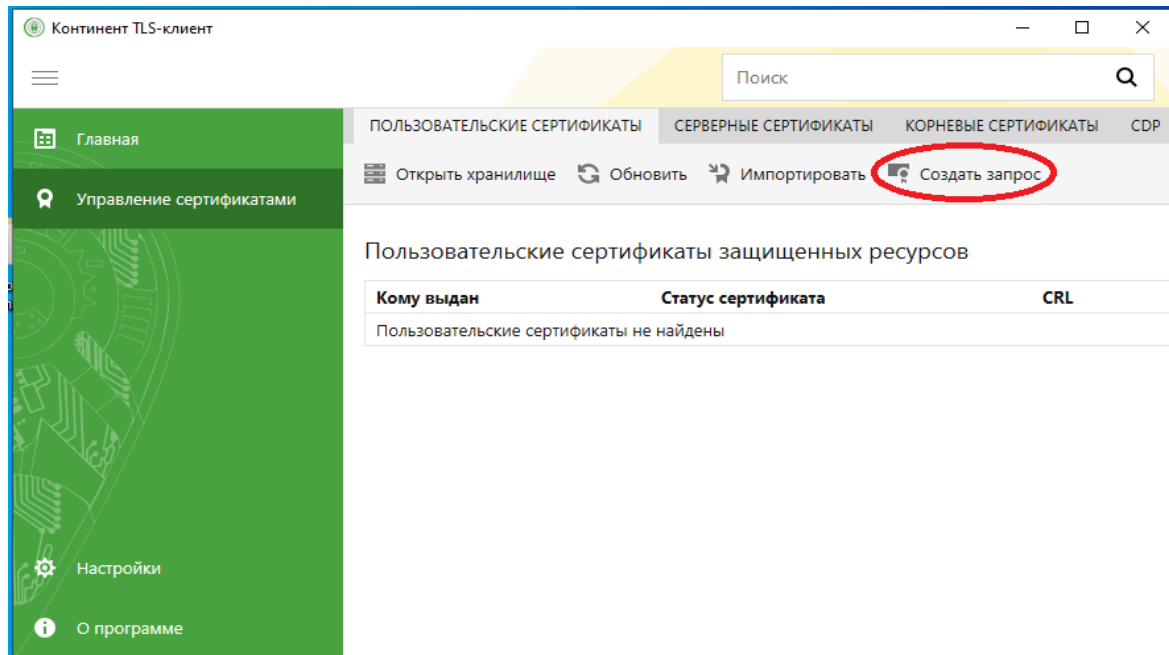


Рис.23

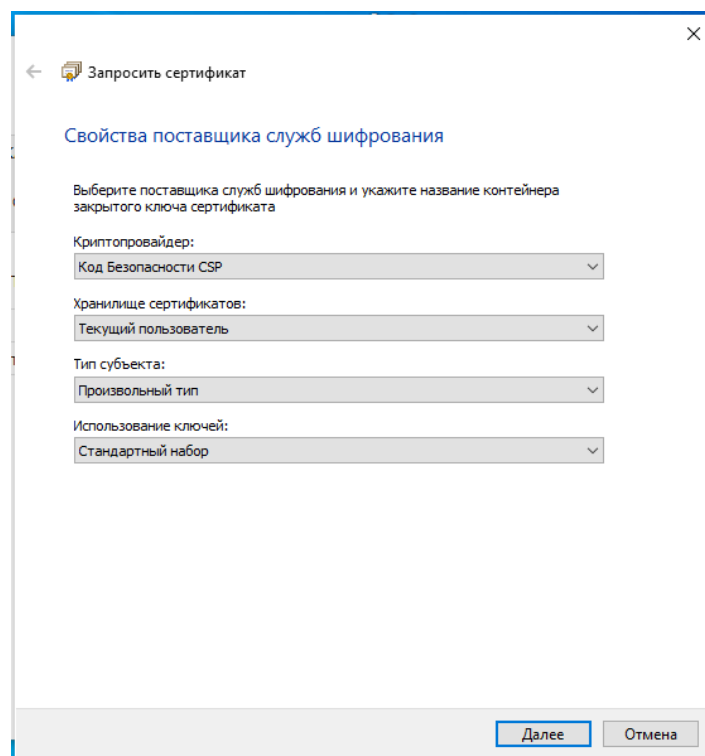


Рис.24

5.1. Заполнить форму «Параметры сертификата пользователя» и нажать «Далее», см. рис.25. Поля обязательные к заполнению можно посмотреть в документе «Правила заполнения полей и применения ключей проверки ЭП» размещенные в разделе «АСОИ ФинЦЕРТ (Документация и ПО Участника)» на информационном портале АСОИ ФинЦЕРТ.

Запросить сертификат

Параметры сертификата пользователя

Заполните обязательные поля для выпуска запроса сертификата пользователя. В полях должны быть указаны полные официальные названия без сокращений.

Фамилия: Имя Отчество:

Общее имя:

Организация:

Подразделение:

Должность:

Страна: Область:

Населенный пункт:

Адрес:

Электронная почта:

ИНН: СНИЛС:

ОГРН:

Рис.25

5.2. В следующем окне необходимо поставить отметки в соответствии с рис.26, указать имя и путь для сохранения запроса сертификата и нажать «Далее».

Запросить сертификат

Имя файла

Имя ключевого контейнера:

Имя файла для запроса сертификата:

Формат файла:
☐ Base64
☒ Двоичные данные

Бланк запроса на сертификат:
☒ Подготовить бланк запроса на сертификат

Рис.26

5.3. В открывшемся окне нажать «Готово», см. рис.27. Отобразится окно для ввода пароля от закрытого ключа. Ввести пароль и нажать «ОК», см. рис.28. (При утере пароля придется получать TLS-сертификат заново.)

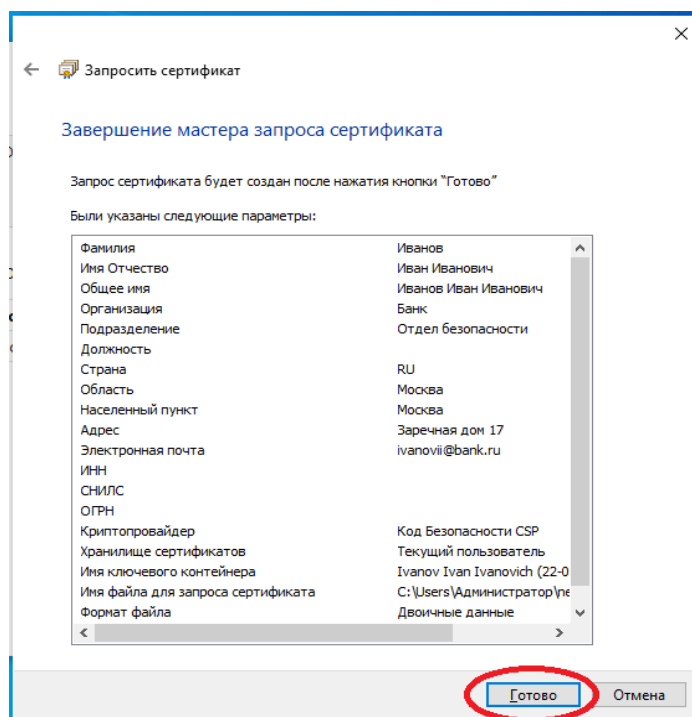


Рис.27

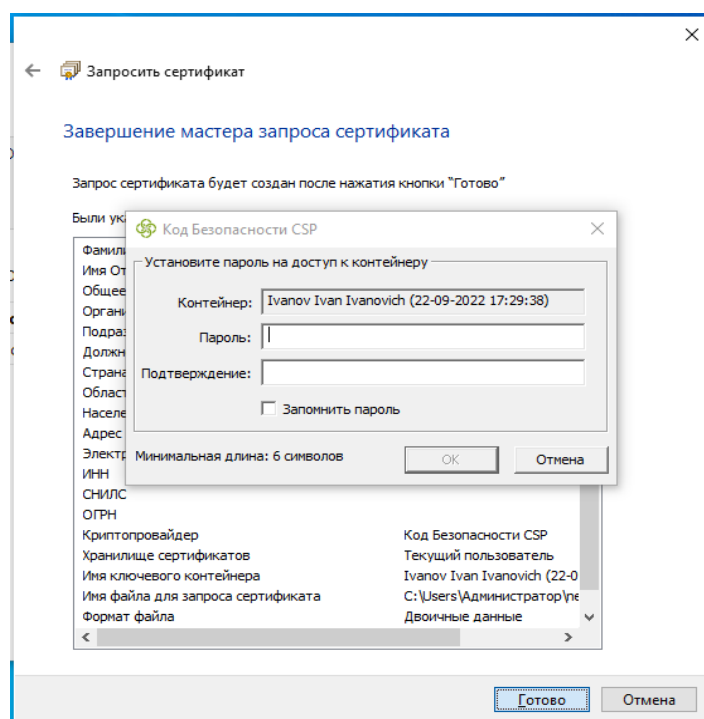


Рис.28

5.4. Далее необходимо выбрать носитель информации, на который будет произведена запись закрытого ключа, см. рис.29. В качестве ключевого носителя можно использовать носитель информации с USB интерфейсом или специальные носители: Rutoken, Etoken (необязательно).

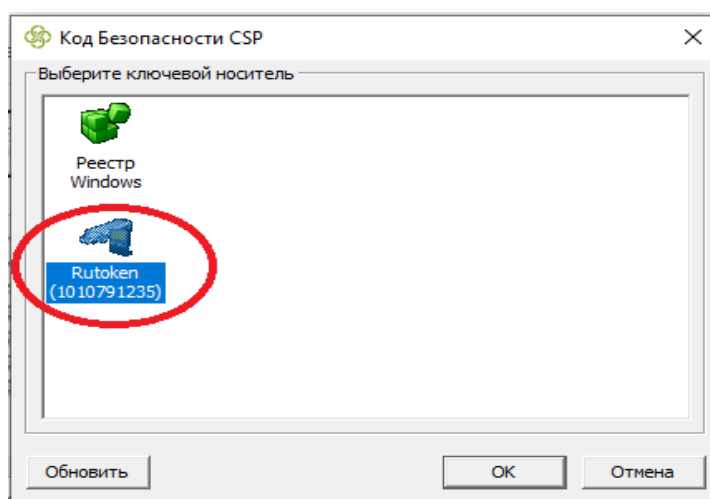


Рис.29

5.5. При использовании специального носителя (Rutoken, Etoken) откроется окно для ввода PIN. Необходимо еще раз ввести пароль и нажать «ОК».

5.6. Далее на экране появится сообщение об успешном создании запроса на сертификат, см. рис.30.

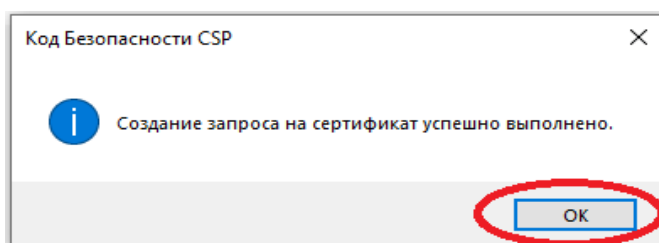


Рис.30

5.7. Владелец ключа необходимо распечатать и подписать печатную форму запроса на сертификат. Печатная форма запроса (в виде HTML-файла) располагается в указанной пользователем папке вместе с запросом на сертификат, см. рис.26. Пример печатной формы, см. рис.31. Запросы в электронной форме (на USB-накопителе) и в виде распечатки направляются в территориальное учреждение Банка России (далее – ТУ БР) с сопроводительным письмом. Образец сопроводительного письма и порядок направления запросов на получение сертификатов приводится в документе «Регламент получения ключевой информации», размещенном на информационном портале АСОИ ФинЦЕРТ. Письмо доставляется в экспедицию ТУ БР любым доступным способом, например, сотрудником организации заявителя, почтовой или курьерской службой.

Иванов Иван Иванович

Заявка на получение в удостоверяющем центре сертификата ключа

В связи с _____
получением мной закрытого ключа, открытого ключа, сертификата ключа, сертификата ключа для подписи, сертификата ключа для шифрования

прошу выдать сертификат ключа для доступа в защищённые сети предприятия участнику информационной системы:

Фамилия, имя, отчество **Иванов Иван Иванович**

Организация **Банк**

Должность _____

Подразделение **ИБ**

Паспорт: серия _____ № _____ выдан _____ дата выдачи _____

Приказом по организации _____ от "____" _____ 201____ г. № _____
 работнику предоставлены полномочия на эксплуатацию _____ (экземпляр приказа прилагается).

Алгоритм открытого ключа: ГОСТ Р 34.10-2012 (256 бит)
 Распечатка значения открытого ключа пользователя:
 04 40 4E 8B 1A 2D 5C 48 BD DB 69 A6 6F 32 D0 26
 7A AC 30 92 CA 0B D9 27 D1 DB 1F B6 B0 3E 48 5A
 3F 76 D6 43 F1 57 6C CE CC 54 22 B3 B0 7B 4B FD
 32 EC 1F 36 80 77 BA AB E9 77 49 98 BE 0B 3D 54
 D7 10

Штамп открытого ключа по алгоритму ГОСТ Р 34.11-2012 (256 бит):
 56 D8 BC 5B 48 EE BF D1 5B A6 54 78 47 69 E6 A3
 34 FF 66 BF 53 00 E1 E9 F7 31 D2 23 E2 C0 3C FE

Алгоритм подписи запроса: ГОСТ Р 34.10-2012 (256 бит)
 Распечатка значения подписи запроса:
 B9 ED 7D A8 B1 32 43 6C 52 AF 41 7D 04 B2 CE 9C
 C0 8D 44 FB 0C 2A E4 3F 94 34 DF D6 28 A2 24 62
 92 EB 6E E4 57 CF 6C 08 33 01 DD CD 53 A7 82 A9
 4A 09 3B 0D 1C C4 47 0A A9 D1 B9 8C A6 71 8A 84

Владелец ключей ЭЦП, сформировавший запрос _____
 Подпись "____" _____ 201____ г.

Поля оставлять
пустыми или удалять

Рис.31

5.8. В корневом разделе накопителя с USB-интерфейсом будет создана папка «topsecretkeys» в которой будет сохранена закрытая (секретная) часть ключа в виде специально подготовленного файла. Указанный файл следует безопасно хранить, не направлять по каналам электронной почты, не направлять в ТУ БР при направлении запроса на сертификат. При утере или компрометации закрытой (секретной) части ключа TLS-сертификат подлежит отзыву.

Генерация закрытого ключа и формирование запроса на получение сертификата в СКЗИ Континент TLS-клиент, с использованием криптопровайдера КриптоПро CSP

Если в вашей организации используется СКЗИ КриптоПро CSP, то Вы должны сгенерировать запрос на сертификат, используя СКЗИ Континент TLS-клиент (в качестве программы для формирования запроса в необходимом формате). Для этого Вам необходимо поверх ранее установленного КриптоПро произвести установку Континент TLS-клиент. В этом случае криптопровайдер от компании «Код безопасности» не будет установлен, и Вы сможете использовать криптосредства КриптоПро CSP.

6. Открыть СКЗИ «Континент TLS-клиент». Перейти в раздел «Управление сертификатами» и на вкладке «Пользовательские сертификаты» нажать «Создать запрос», см. рис.23.

6.1. В открывшемся окне заполнить форму «Параметры сертификата пользователя» и нажать «Далее», см. рис.32.

Рис.32

6.2. При генерации запроса на сертификат в СКЗИ Континент TLS-клиент с установленным на ПК КриптоПро, обратите внимание на опцию выбора криптопровайдера, см. рис.33.

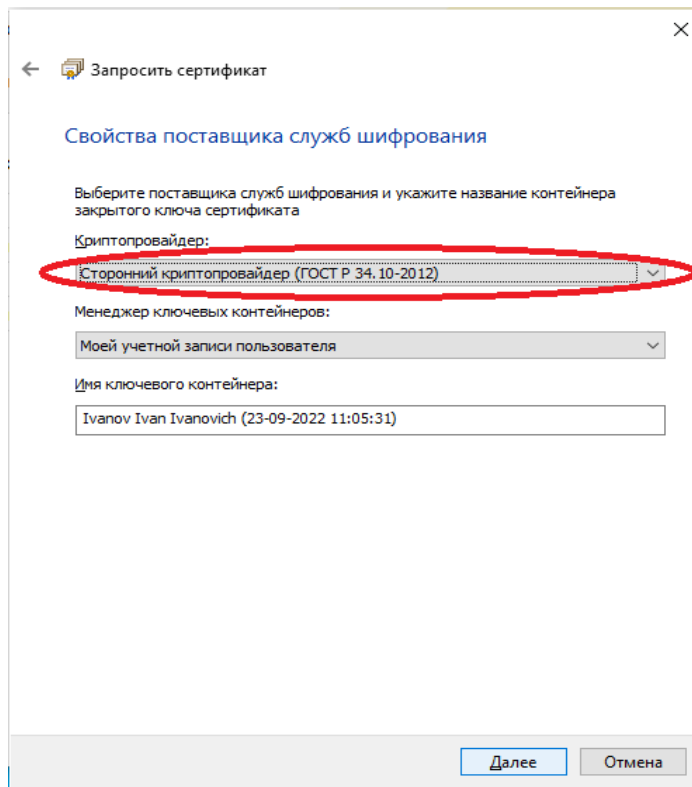


Рис.33

6.3. В следующем окне необходимо поставить отметки в соответствии с рис.34 и нажать «Далее».

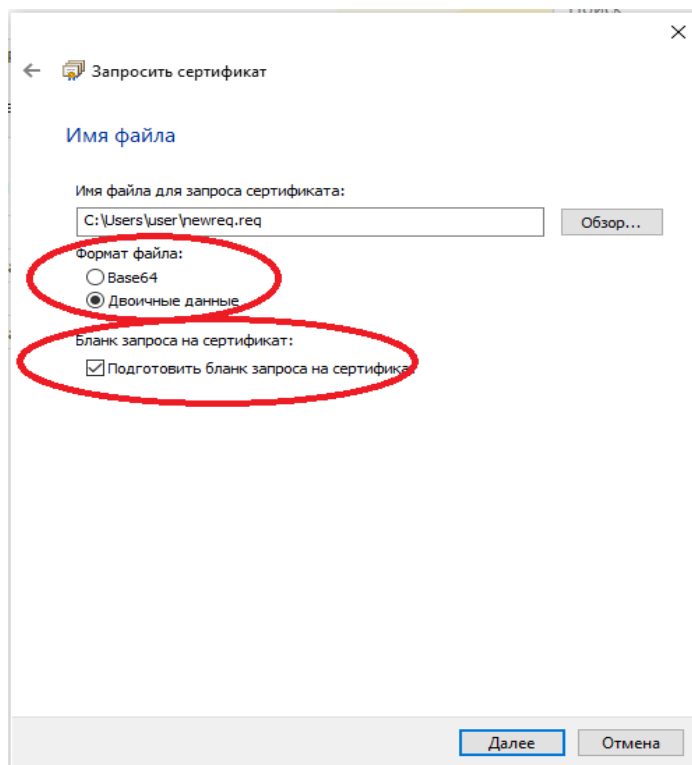


Рис.34

6.4. Для дальнейшей генерации необходимо пройти датчик случайных чисел, см. рис.35.

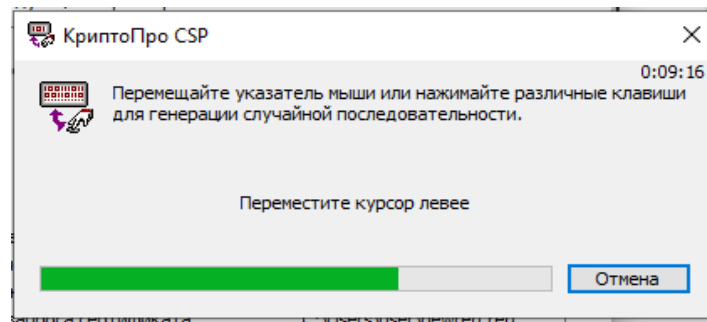


Рис.35

6.5. Выбрать носитель из списка, см. рис.36.

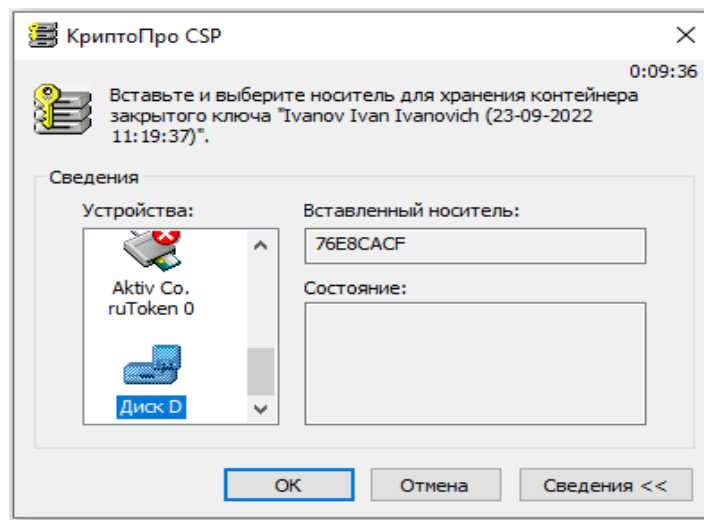


Рис.36

6.6. Ввести пароль и нажать «ОК». На экране появится сообщение об успешном создании запроса на сертификат, см.рис.37-38.

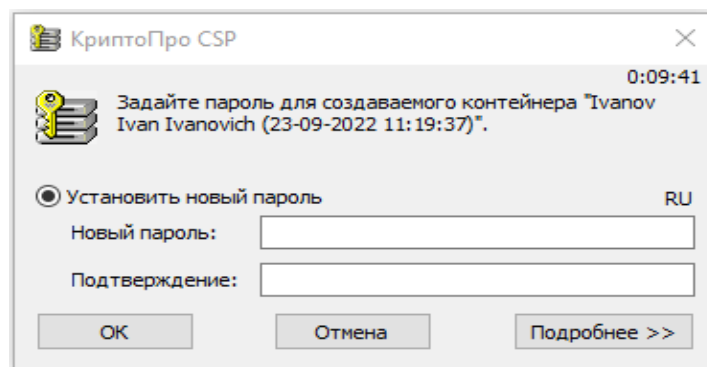


Рис.37

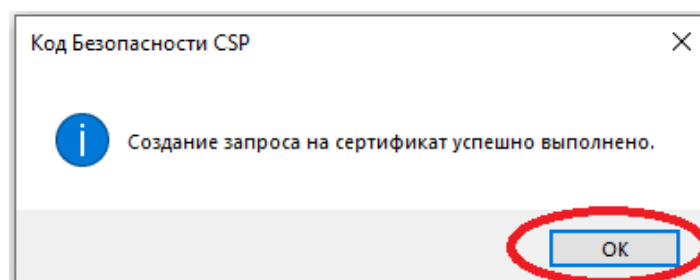


Рис.38

6.7. Владелец ключа необходимо распечатать и подписать печатную форму запроса на сертификат. Печатная форма запроса (в виде HTML-файла) располагается в указанной пользователем папке вместе с запросом на сертификат, см. рис.34. Пример печатной формы, см. рис.39. Запросы в электронной форме (на USB-накопителе) и в виде распечатки направляются в ТУ БР с сопроводительным письмом. Образец сопроводительного письма и порядок направления запросов на получение сертификатов приводится в документе «Регламент получения ключевой информации», размещенном на информационном портале АСОИ ФинЦЕРТ. Письмо доставляется в экспедицию ТУ БР любым доступным способом, например, сотрудником организации заявителя, почтовой или курьерской службой

Иванов Иван Иванович

Заявка на получение в удостоверяющем центре сертификата ключа

В связи с _____,

прошу выдать сертификат ключа для доступа в защищённые сети предприятия участнику информационной системы:

Фамилия, имя, отчество **Иванов Иван Иванович**

Организация **Банк**

Должность _____

Подразделение **ИБ**

Паспорт: серия _____ № _____ выдан _____ дата выдачи _____

Приказом по организации _____ от "____" _____ 201 ____ г. № _____

работнику предоставлены полномочия на эксплуатацию _____ (экземпляр приказа прилагается).

Алгоритм открытого ключа: ГОСТ Р 34.10-2012 (256 бит)
 Распечатка значения открытого ключа пользователя:
 04 40 4E 8B 1A 2D 5C 48 BD DB 69 A6 6F 32 D0 26
 7A AC 30 92 CA 0B D8 27 D1 DB 1F B6 B0 3E 48 5A
 3F 76 D6 43 F1 57 6C CE CC 54 22 B3 B0 7B 4B FD
 32 EC 1F 36 80 77 BA AB E9 77 49 98 BE 0B 3D 54
 D7 10

Штамп открытого ключа по алгоритму ГОСТ Р 34.11-2012 (256 бит):
 56 D8 BC 5B 48 EE BF D1 5B A6 54 78 47 65 E6 A3
 34 FF 66 BF 53 00 E1 E9 F7 31 D2 23 E2 C0 3C FE

Алгоритм подписи запроса: ГОСТ Р 34.10-2012 (256 бит)
 Распечатка значения подписи запроса:
 B9 ED 7D A8 B1 32 43 6C 52 AF 41 7D 04 B2 CE 9C
 C0 8D 44 FB 0C 2A E4 3F 94 34 DF D5 28 A2 24 62
 92 EB 6E E4 57 CF 6C 08 33 01 DD 0D 53 A7 82 A9
 4A 09 3B 0D 1C C4 47 0A A9 D1 B9 8C A6 71 8A 84

Владелец ключей ЭЦП, сформировавший запрос _____

Подпись "____" _____ 201 ____ г.

Поля оставлять
пустыми или удалять

Рис. 39

6.8. В корневом разделе накопителя с USB-интерфейсом будет создана папка вида «IVANOV.000» в которой будет сохранена закрытая (секретная) часть ключа в виде набора специально подготовленных файлов с расширением «*.key». Указанные файлы следует безопасно хранить, не направлять по каналам электронной почты, не направлять в ТУ БР при направлении запроса на сертификат. При утере или компрометации закрытой (секретной) части ключа TLS-сертификат подлежит отзыву.

Установка пользовательского сертификата

7. После получения в ТУ БР пользовательского сертификата необходимо произвести его установку. В комплекте с пользовательским сертификатом ТУ БР предоставляет сертификаты корневого центра сертификации и подчиненного центра сертификации, который необходимо установить. Как устанавливать корневые и серверные сертификаты описано выше, см. рис.10-15. По аналогии необходимо добавить сертификат подчиненного центра сертификации в раздел «Промежуточные центры сертификации», см. рис.40.

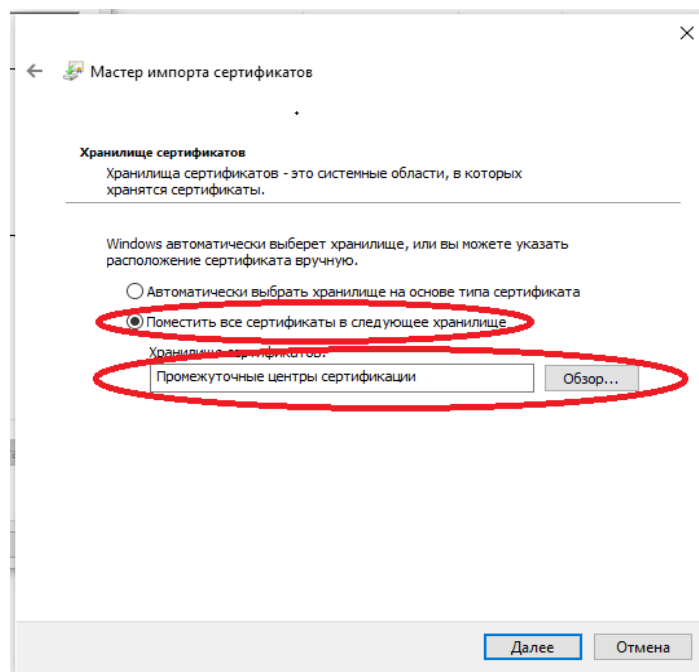


Рис.40

7.1. Для установки пользовательского сертификата необходимо открыть СКЗИ и выполнить соответствующую команду. Процедура установки аналогична для СКЗИ «Континент TLS-клиент» и КриптоПро. В случае «Континент TLS-клиент» необходимо: вставить носитель с закрытым ключом, перейти в раздел «Управление сертификатами» и на вкладке «Пользовательские сертификаты» нажать «Импортировать». см. рис.41.

При использовании КриптоПро необходимо вставить носитель с закрытым ключом, перейти в раздел «Сервис» и выбрать команду «Установить личный сертификат...», см. рис. 42.

Далее приводится последовательность шагов при работе в СКЗИ «Континент TLS-клиент».

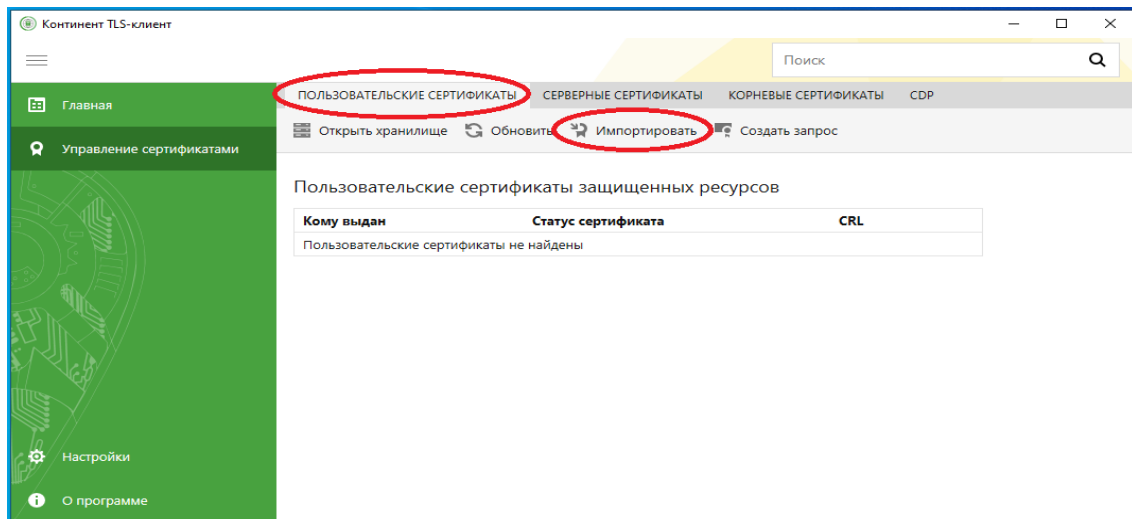


Рис.41

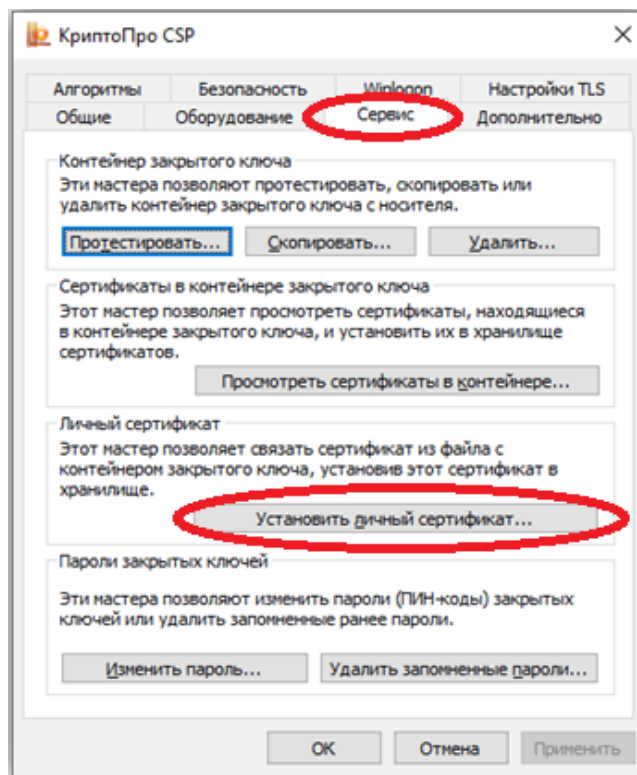


Рис.42

7.2. В открывшемся окне нажать «Обзор», выбрать пользовательский сертификат и нажать «Далее», см. рис.43.

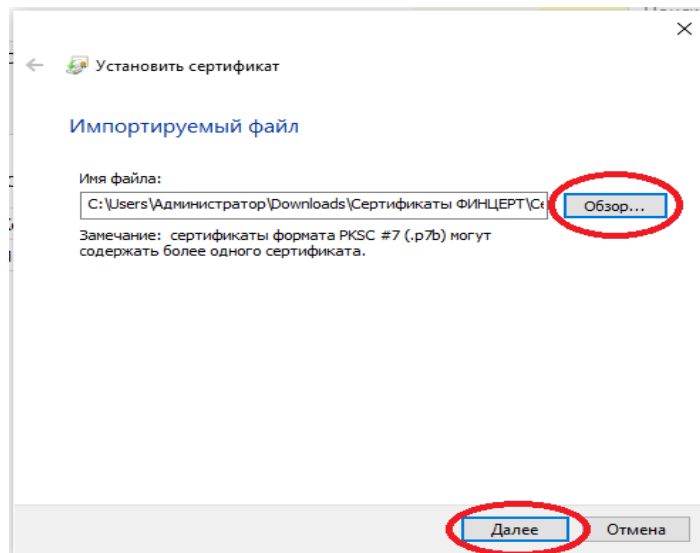


Рис.43

7.3. В следующем окне поставить отметку в соответствии с рис.44 и нажать «Далее».

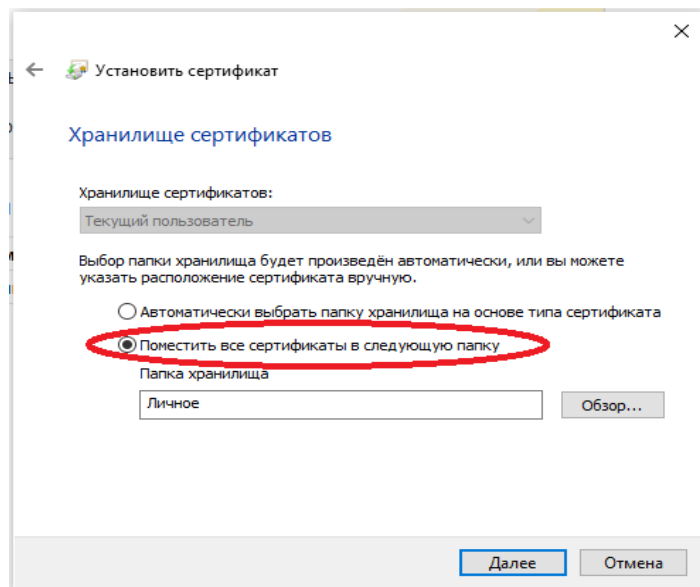


Рис. 44

7.4. Затем выбрать носитель с закрытым ключом и нажать «Далее», см. рис.45.

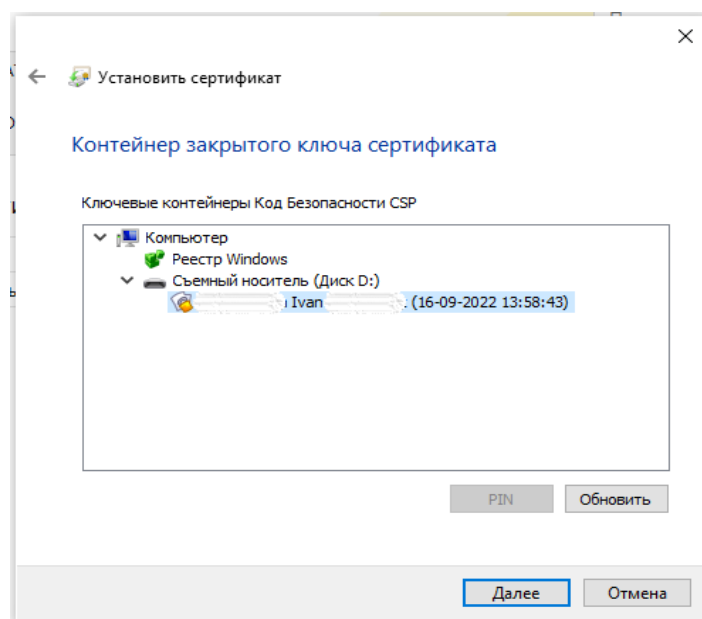


Рис.45

7.5. Ввести пароль и нажать «ОК», см. рис.46.

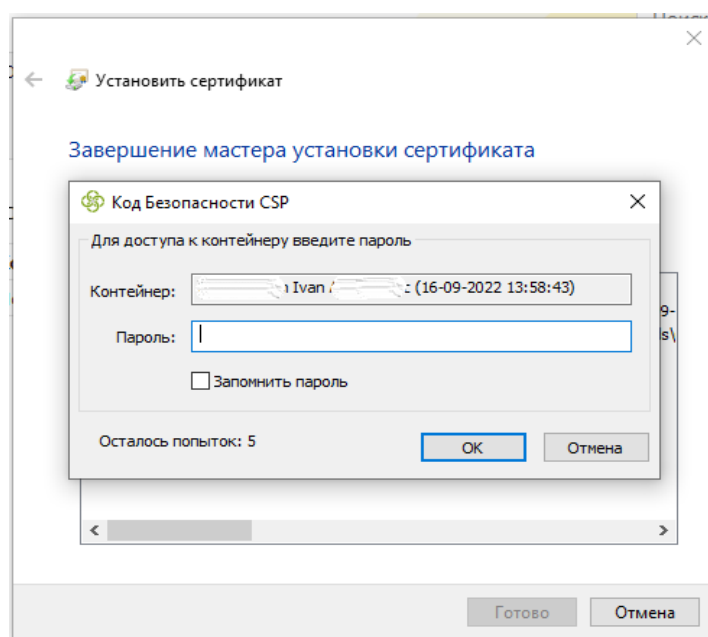


Рис.46

7.6. Для завершения установки сертификата нажать «Готово» и в появившемся окне – «ОК», см. рис.47-48.

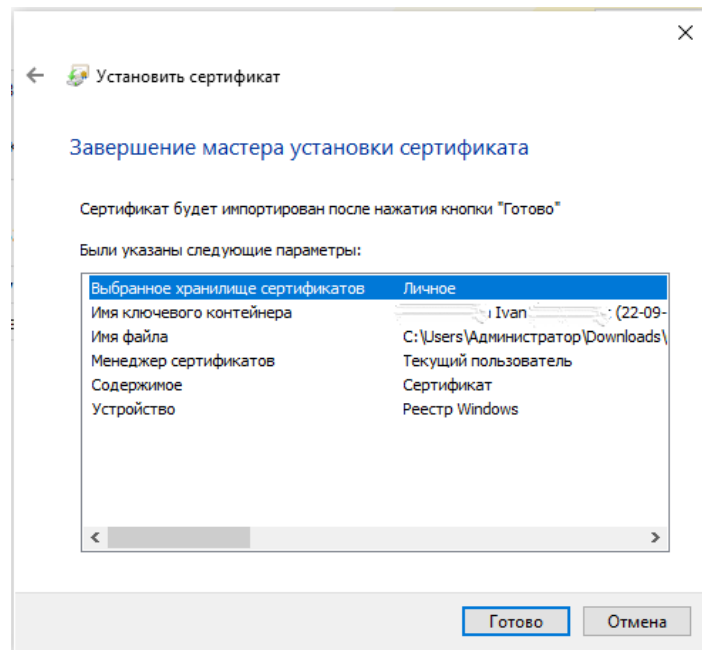


Рис.47

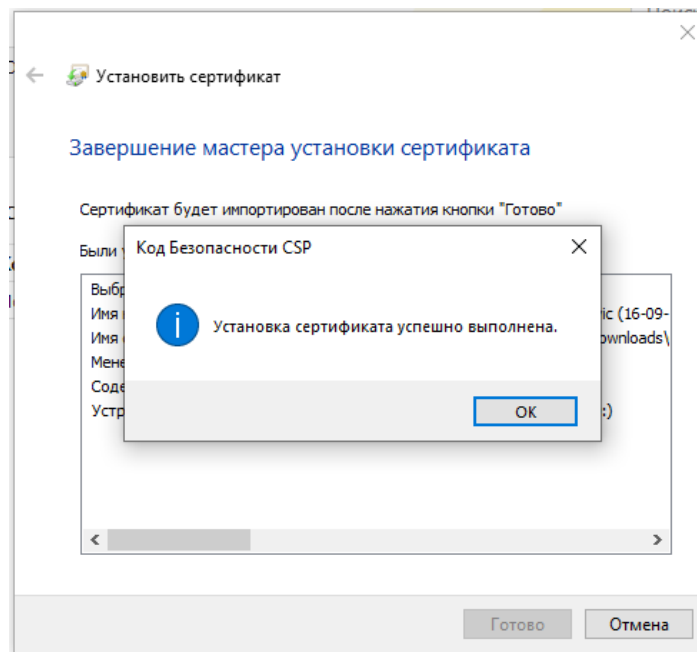


Рис.48

7.7. После установки пользовательского сертификата и перехода по адресу lk.fincert.cbr.ru пользователю будет предложено выбрать нужный сертификат для подключения к системе, см. рис.49. (При использовании «Континент TLS-клиент» в настройках программы можно выбрать нужный сертификат для использования по умолчанию, что позволит не выбирать каждый раз сертификат для подключения к АСОИ ФинЦЕРТ).

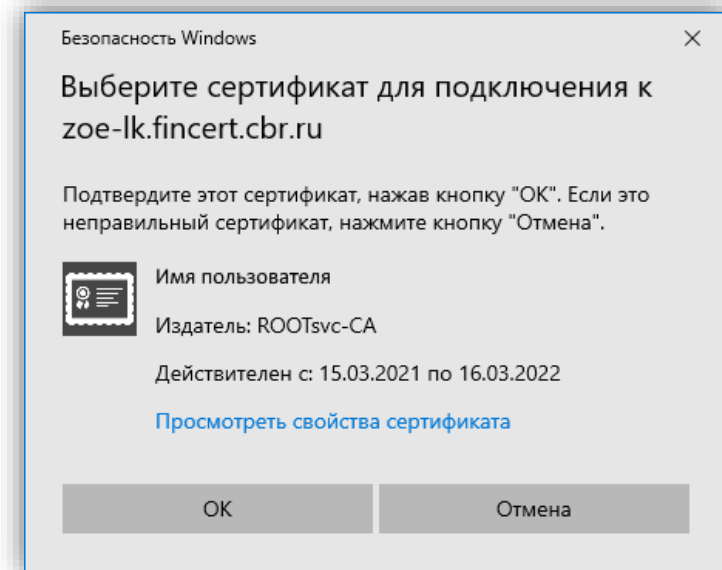


Рис.49

При выполнении всех шагов в строгой последовательности Вы сможете зайти в Личный кабинет Участника АСОИ ФинЦЕРТ! См. рис.50.

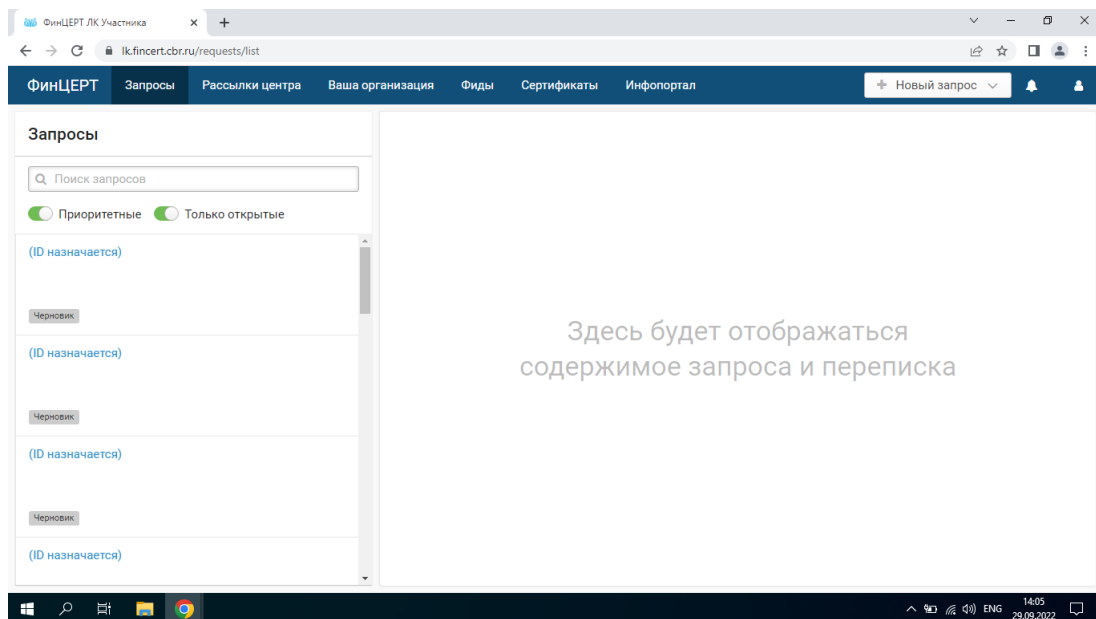


Рис.50

Проблемы при подключении к АСОИ ФинЦЕРТ у пользователей возникают по следующим причинам:

- невнимательность при установке сертификатов на компьютер;
- сетевые проблемы при прохождении трафика (межсетевые экраны, прокси, VPN-соединение, контроль трафика антивирусом и т.п.);

- некорректная работа СКЗИ (в т.ч. использование неподходящего браузера при использовании СКЗИ КриптоПро, установка другого криптопровайдера и СКЗИ на одном компьютере, обновление других программ, влияющих на работу СКЗИ и т.п.).

В том случае, если у Вас возникли какие-то сложности, рекомендуем также ознакомиться с документом «Ответы на вопросы Участников по получению TLS-сертификатов (FAQ)» (файл размещен на информационном портале АСОИ ФинЦЕРТ, направляется в составе стартового комплекта документов.)